2015

The View from Inside the NSA Review Group

Geoffrey R. Stone

THE VIEW FROM INSIDE THE NSA REVIEW GROUP†

*Geoffrey R. Stone**

ABSTRACT

This Article offers a glimpse inside the President's Review Group on Intelligence and Communications Technologies, documents University of Chicago Law School Dean Geoffrey Stone's thoughts leading up to and after his time on the Review Group, and provides his insight on three main areas of the Review Group's final report.

TABLE OF CONTENTS

In August 2013, I was sitting in my office working on a book, minding my own business, when I received a phone call from a former student, Lisa

† Parts of this Article are adopted from previous articles I wrote in The University of Chicago Magazine and the Daily Beast. *See* Geoffrey R. Stone, *Into the Breach*, THE UNIVERSITY OF CHICAGO MAGAZINE, Feb. 2015, http://mag.uchicago.edu/law-policy-society/breach; Geoffrey R. Stone, *Here's Who Should Watch the Watchmen*, THE DAILY BEAST (April 23, 2014), http://www.thedailybeast.com/articles/2014/04/23/here-s-who-should-watch-the-watchmen.html.

* Interim Dean and Edward H. Levi Distinguished Service Professor, The University of Chicago.

Monaco, who was then serving as Assistant Attorney General for National Security. Lisa told me that, in the wake of Edward Snowden's revelations,[1] President Barack Obama was in the process of appointing a five-member Review Group to evaluate the nation's foreign intelligence programs.[2] She asked if I might be willing to serve as a member of the President's Review Group.

My first thought, quite literally, was "oh, shit." This would undoubtedly be a hugely time-consuming task that would distract me from my writing and, like most government committees, would produce a report that would inevitably disappear into somebody's desk and have no impact at all.

When the President asks though, you do not say no, especially when you were the person who, as Dean of the University of Chicago Law School, appointed him to the faculty. So, I kept my first thought to myself and replied, "Sure, happy to do it," confident though that I had an ace in the hole that would prevent me from serving.

I knew I would need a top-secret clearance, and I figured there was more than enough in my background to preclude that. But, somewhat to my dismay, I had done nothing disqualifying. I expeditiously received a top-secret security clearance and was soon hustled off to Washington to meet in the White House Situation Room with President Obama, National Security Advisor Susan Rice, and several other high-level government officials who would get us started on our journey.

I.

On the flight to that first meeting, I reflected about what I might contribute to this process. As I thought about the problem of foreign intelligence surveillance in the years since 9/11, I focused on three very different perspectives.

First, I thought about the daunting challenge of keeping the nation safe in the face of twenty-first-century threats. Traditionally, both in the criminal

1. Mark Mazzetti & Michael S. Schmidt, *Ex-Worker at C.I.A. Says He Leaked Data on Surveillance*, N.Y. TIMES (June 9, 2013), http://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html?pagewanted=all&_r=0.

2. Press Release, The White House, Statement by the Press Secretary on the Review Group on Intelligence and Communications Technology (Aug. 27, 2013), https://www.whitehouse.gov/the-press-office/2013/08/27/statement-press-secretary-review-group-intelligence-and-communications-t.

justice system and in the context of international relations, we rely principally, on deterrence to keep ourselves safe.[3] We tell potential criminals and potential international enemies that if you mess with us, we will make you pay.[4] Deterrence is essential to safety.[5] But in the contemporary world of international terrorism, deterrence is largely irrelevant.[6] Those who would attack us are not afraid to die, and because they are not associated with any nation-state, there is no one against whom we can retaliate.[7] In short, deterrence is nonexistent. In such circumstances, the only realistic way to keep ourselves safe is advanced detection so we can prevent terrorist attacks from occurring.[8]

Moreover, I thought, as demonstrated by the events of 9/11, international terrorists today can inflict massive damage, using not only conventional but possibly also chemical, biological, and even nuclear weapons.[9] Such attacks can not only cost billions of dollars of damage and cause thousands of deaths, but they can also change our culture in fundamental ways by leading us to sacrifice ever more of our civil liberties and privacy in the

3. *See, e.g.*, ARTHUR W. CAMPBELL, LAW OF SENTENCING § 2:2 (2014); Alex Winter, *Contemporary Deterrence Theory and Counterterrorism: A Bridge too Far?*, 47 N.Y.U. J. INT'L L. & POL. 439, 439–40 (2015).

4. *See* CAMPBELL, *supra* note 3.

5. *See id.*

6. Leora Bilsky, *Suicidal Terror, Radical Evil, and the Distortion of Politics and Law*, 5 THEORETICAL INQUIRIES L. 131, 140 (2004); Austin Long, *Deterrence: The State of the Field*, 47 N.Y.U. J. INT'L L. & POL. 357, 358 (2015).

7. *See* President George W. Bush, Graduation Speech at West Point, (June 1, 2002), http://georgewbush-whitehouse.archives.gov/news/releases/2002/06/20020601-3.html ("For much of the last century, America's defense relied on the Cold War doctrines of deterrence and containment. In some cases, those strategies still apply. But new threats also require new thinking. Deterrence—the promise of massive retaliation against nations—means nothing against shadowy terrorist networks with no nation or citizens to defend."); *see also* Riaz Hassan, *What Motivates the Suicide Bombers?*, YALE GLOBAL ONLINE (Sept. 3, 2009), http://yaleglobal.yale.edu/content/what-motivates-suicide-bombers-0.

8. *See* Andrew Peterson, *Addressing Tomorrow's Terrorists*, 2 J. NAT'L SECURITY L. & POL'Y 297, 302 (2008) ("After 9/11, the government realized that it could not wait for other terrorist attacks to occur. Accordingly, [it] shifted its focus from the prosecution of crimes already committed to the prevention of future terrorist acts.").

9. *See* 50 U.S.C. § 1801(p)(1)–(4) (2012) (defining weapons of mass destruction within the same subchapter as "international terrorism" to include explosives, poisonous chemicals, biological agents, and radioactivity).

quest for national security.[10] The costs of failing to prevent such attacks, I thought, would be staggering.

Even worse, I thought, twenty-first-century terrorists operate within a global communications network that enables them to communicate with one another secretly across the globe at the speed of light.[11] The challenge of preventing these attacks requires our government to identify and stop terrorists in advance before they are able to strike.[12]

All of this left me daunted. I recalled that, in the years after 9/11, a former cabinet member, James Baker, suggested a vivid analogy about what it felt like to be charged with "the task of stopping" the next terrorist attack.[13] It felt, he said, like being:

> [A] goalie in a soccer game who "must stop every shot, for the enemy wins if it scores a single goal." The problem, Baker says, "is that the goalie cannot see the ball—it is invisible. So are the players—he doesn't know how many there are, or where they are, or what they look like. He also doesn't know where the sidelines are—they are blurry and constantly shifting, as are the rules of the game itself." The invisible players might shoot the invisible weapon "from the front of the goal, or from the back, or from some other direction—the goalie just doesn't know."[14]

In short, the only way the goalie can stop a goal is by watching the movements of the blades of grass.[15] Reflecting on that analogy left me with a very sober sense of the challenge facing our nation's intelligence agencies. Quite simply, if the government was too cautious in its efforts to identify and locate would-be terrorists before they strike, the consequences for the nation could be disastrous.

The second perspective from which I thought about these issues on that first flight to Washington drew on my own personal commitment to the need

10. *See* Todd Landman, *Imminence and Proportionality: The U.S. and U.K. Responses to Global Terrorism*, 38 CAL. W. INT'L L. J. 75, 87–88 (2007).

11. James A. Lewis, *The Internet and Terrorism*, 99 AM. SOC'Y INT'L L. PROC. 112, 113 (2005).

12. *See* K. A. Taipale, *The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance*, 9 YALE J.L. & TECH. 128, 138–39 (2007) (discussing the need for surveillance and analysis of global communications in order to preempt terrorist attacks).

13. JACK GOLDSMITH, THE TERROR PRESIDENCY 73 (W. W. Norton & Co. ed., 2007).

14. *Id.* (quoting Interview with James A. Baker).

15. *See id.*

to be especially vigilant in our protection of civil liberties and personal privacy. As a long-time civil libertarian, member of the American Civil Liberties Union's National Advisory Board, and former chair of the board of the American Constitution Society, I have a long track record in the defense of individual freedom.[16] Indeed, I assumed that was at least part of the reason why President Obama asked me to serve on the Review Group. The challenge, I knew, would be to find a way to preserve robust protection of our rights and liberties, while at the same time keeping our nation safe. This would be no easy task.

The third perspective that was very much on my mind that day was my understanding that, in times of national crisis, there is a natural and, indeed, inevitable tendency to overreact to perceived dangers at the expense of individual freedom.[17] The inclination is, quite simply, "better be safe than sorry."[18] This was so, for example: (1) at the end of eighteenth century when the nation enacted the Alien and Sedition Acts in the face of a feared war with France; (2) during the Civil War when Abraham Lincoln aggressively suspended the writ of habeas corpus; (3) during World War I when the Wilson Administration secured the enactment of the Espionage and Sedition Acts and used those laws to suppress virtually all criticism of the war and the draft; (4) during World War II when the Roosevelt Administration ordered the internment of 120,000 persons of Japanese descent, the vast majority of whom were American citizens; (5) during the Cold War when our nation unleashed an array of programs at every level of government designed to prosecute, blacklist, and humiliate thousands of American citizens because of their supposed "Communist" leanings; and (6) during the Vietnam War when J. Edgar Hoover, Lyndon Johnson, and Richard Nixon initiated wide-ranging and illegal domestic surveillance programs in order to "expose, disrupt, and otherwise neutralize" their political opponents.[19]

16. *See Geoffrey R. Stone*, U. CHI. L. REV., http://www.law.uchicago.edu/faculty/stone-g (last viewed July 9, 2015); *see also* Geoffrey R. Stone, *A Lawyer's Responsibility: Protecting Civil Liberties in Wartime*, 22 WASH. U. J.L. & POL'Y 47, 53–55 (2006) [hereinafter Stone, *Lawyer's Responsibility*]; Geoffrey R. Stone, *Civil Liberties in Wartime*, SHARE AMERICA (April 6, 2015), http://share.america.gov/civil-liberties-wartime/ [hereinafter Stone, *Wartime*].

17. *See* Stone, *Lawyer's Responsibility*, *supra* note 16, at 47–52; Stone, *Wartime*, *supra* note 16 ("[W]ar breeds fear and fear breeds repression.").

18. *See* Stone, *Wartime*, *supra* note 16.

19. *See, e.g.*, GEOFFREY R. STONE, PERILOUS TIMES: FREE SPEECH IN WARTIME FROM SEDITION ACT OF 1798 TO THE WAR ON TERRORISM 12–13 (2004) [hereinafter STONE, PERILOUS TIMES]; CHURCH COMMITTEE DETAILED STAFF REPORTS ON

This was an issue I had thought much about during my career,[20] and I was acutely aware of the danger that, human nature being what it is, it was highly likely that in our response to the tragedy of 9/11 we had similarly overreacted. My concern was not that we had nothing to fear, but that given past experience, in designing our response to the threat of terrorism we had failed to strike an appropriate balance between the fundamental values of national security and personal liberty. As I deplaned, I thought to myself: "This is the issue."

II.

In our first meeting in the Situation Room later that afternoon, President Obama told us that he wanted the Review Group to serve as an independent body that would advise him about how best to strike an appropriate balance between protecting national security and preserving civil liberties, and how best to restore public trust in our nation's intelligence agencies in the wake of Edward Snowden's disclosures.[21] He made it very clear that he wanted us to be rigorous, tough-minded, and honest in every way.

We were a diverse group in terms of our professional backgrounds, experiences, and ways of thinking about these issues. There was Michael Morell, who had spent his career with the Central Intelligence Agency (CIA), including two stints as acting director;[22] Richard Clarke, a veteran of the State and Defense Departments in four presidential administrations and an expert in cybersecurity;[23] Peter Swire, a professor at Georgia Tech who had

INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS: BOOK III, FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, United States Senate, S. Rep. No. 94-755 (1976) [hereinafter CHURCH COMMITTEE REPORT]; *see also generally* ROBERT JUSTIN GOLDSTEIN, POLITICAL REPRESSION IN MODERN AMERICA: FROM 1870 TO THE PRESENT (1978); ATHAN THEOHARIS, SPYING ON AMERICANS: POLITICAL SURVEILLANCE FROM HOOVER TO THE HUSTON PLAN (1978).

20. *See, e.g.*, Stone, *Lawyer's Responsibility*, *supra* note 16, at 47–52; Stone, *Wartime*, *supra* note 16.

21. *See* THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD 10–13 (2013) [hereinafter REVIEW GROUP].

22. *See Executive Profile: Michael J. Morell*, BLOOMBERG BUSINESS, http://www.bloomberg.com/research/stocks/private/person.asp?personId=42732503&privcapId=275789 (last visited July 22, 2015).

23. *See Biography*, RICHARD A. CLARKE, http://www.richardaclarke.net/bio.php (last visited July 22, 2015).

served in both the Clinton and Obama administrations as an expert on issues of privacy and information technology;[24] and Cass Sunstein, one of our nation's most distinguished legal scholars who had just finished a stint in the Office of Management and Budget during the Obama administration.[25] And then there was me, a constitutional law professor at the University of Chicago and a self-professed civil libertarian.[26] It was quite clear, given the makeup of the Review Group, that we would agree on nothing. As Susan Rice later commented to us, we were "five highly egotistical, high-testosterone guys" who were being "thrown in a room together, with nobody in charge, and expected to solve a set of intractable problems."

Yet, what happened was exactly that. As we spent five months together, working three or four days each week in a secure facility in our nation's capital, we came to trust, respect, and learn from one another so much that—to our amazement—we eventually produced 46 unanimous recommendations.[27] These were not unanimous in the sense of, "I'll give you this one if you give me that one," but in the sense that we all agreed on every recommendation that the Review Group made to the President in our 300-page report.[28]

None of us would have imagined that was possible when we began.

III.

I discovered on the first day that I did not know anything. Unlike the other four members, who had extensive experience in government, I had none except for a year as a law clerk to a Supreme Court Justice 40 years earlier. My inexperience immediately became apparent as I encountered the flood of acronyms. Nary a sentence was uttered where somebody did not say

24. *See Peter Swire*, PETER SWIRE, http://peterswire.net/ (last visited July 9, 2015).

25. *See Cass R. Sunstein*, HARVARD LAW SCHOOL, http://hls.harvard.edu/faculty/directory/10871/Sunstein (last visited July 9, 2015); *see also* John M. Border, *Powerful Shaper of U.S. Rules Quits, With Critics in Wake*, N.Y. TIMES (Aug. 3, 2012), http://www.nytimes.com/2012/08/04/science/earth/cass-sunstein-to-leave-top-regulatory-post.html.

26. *See Geoffrey R. Stone*, *supra* note 16.

27. *See* RICHARD A. CLARKE, MICHAEL J. MORELL, GEOFFREY R. STONE, CASS R. SUNSTEIN, & PETER SWIRE, THE NSA REPORT: LIBERTY AND SECURITY IN A CHANGING WORLD: THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES xxv–xli (2014) [hereinafter, CLARKE ET AL., NSA REPORT].

28. *See generally id.*; REVIEW GROUP, *supra* note 21.

"DARPA" or "NIST" or "PCLOB" or some other acronym that was completely unknown to me.[29] I had no idea what they were talking about.

With some sense of mortification, I raised my hand and said, "Excuse me, what does that mean?" I quickly decided that I was not going to be able to live with raising my hand all the time, so I found myself busily scribbling down acronyms hoping eventually to figure out what they meant. By the end of the first week, I had a list of several dozen I had never heard of before. I Googled them and wrote down the full names. I started to memorize them, but after about six, I realized it was not going to happen. That captures, in microcosm, the experience of being thrown into a world that was strange for each of us in different ways, but probably more for me than anyone else.[30]

We were quickly overwhelmed with requests for meetings. Over the course of the next several months we met not only with President Obama on several occasions but also with the (1) House and Senate Intelligence and Judiciary Committees; (2) National Security Advisor Susan Rice; (3) NSA Director General Keith Alexander; (4) a dozen members of the Senate and House Intelligence and Judiciary Committees individually; (5) high-level officials in the NSA, the CIA, and the FBI; (6) representatives of the Departments of State, Defense, Homeland Security, Commerce, and Treasury; (7) the former Chief Judge of the Foreign Intelligence Surveillance Court (FISC); (8) representatives of the European Union; (9) representatives of more than 25 private organizations ranging from the ACLU, Human Rights Watch, and the Reporters Committee for Freedom of the Press to Google, Facebook, and Yahoo; and (10) many, many more. It was an intensive, exhaustive, and at times exhausting listening and learning process. It was invaluable.

Because much of what we were dealing with was classified, members of the Review Group could not examine documents or even have discussions about what we had learned outside of a secure facility. That meant that I

29. DARPA is the acronym for the Defense Advanced Research Projects Agency. *See About DARPA*, DARPA, http://www.darpa.mil/about-us/about-darpa (last visited July 22, 2015). NIST is the acronym for the National Institute for Standards and Technology. *About NIST*, NAT'L INST. FOR STANDARDS AND TECH., http://www.nist.gov/public_affairs/nandyou.cfm (last visited Feb. 25, 2015). PCLOB is the Privacy and Civil Liberties Oversight Board. *About the Board*, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, http://www.pclob.gov/about-us.html (last visited July 9, 2015).

30. When we finished our task, I gave all members of the team, including the nine extraordinary staff members assigned to assist us, a souvenir sweatshirt that included, on the back, a list of 54 acronyms. It was an in-joke at my expense.

couldn't work on our report from my home or office in Chicago. On weekends, I had to go to a secure facility at the FBI field office in Chicago.

It was like being in a cave for five months. Everything was consumed with the fascinating and demanding work of producing our final 300-page report.

IV.

Before turning to specific recommendations, I should offer two general observations. The first concerns the NSA. "From the outset, I approached my responsibilities as a member of the Review Group with great skepticism about the NSA."[31] I assumed that the most problematic surveillance programs that Edward Snowden had recently brought to light were the result of an NSA run amok. That it had instituted these programs on its own, without lawful authorization, and without the knowledge or oversight of the Congress, the judiciary, or the White House. I could not have been more wrong. As I said in a speech to the NSA:

> I came away from my work on the Review Group with a view of the NSA that I found quite surprising. Not only did I find that the NSA had helped to thwart numerous terrorist plots against the United States and its allies in the years since 9/11, but I also found that it is an organization that operates with a high degree of integrity and a deep commitment to the rule of law.
>
> Like any organization dealing with extremely complex issues, the NSA on occasion made mistakes in the implementation of its authorities, but it invariably reported those mistakes upon discovering them and worked conscientiously to correct its errors. The Review Group found no evidence that the NSA had knowingly or intentionally engaged in unlawful or unauthorized activity. To the contrary, it has put in place carefully-crafted internal procedures to ensure that it operates within the bounds of its lawful authority.
>
> This is not to say that the NSA should have had all of the authorities it was given. The Review Group found that many of the programs undertaken by the NSA were highly problematic and much in need of reform. But the responsibility for directing the NSA to carry out those programs rests not with the NSA, but with the Executive Branch, the

31. Geoffrey Stone, *What I Told the NSA*, HUFFINGTON POST (March 21, 2014), http://www.huffingtonpost.com/geoffrey-r-stone/what-i-told-the-nsa_b_5065447.html [hereinafter Stone, *What I Told*].

> Congress, and the FISC, which authorized those programs—sometimes without sufficient attention to the dangers they posed to privacy and civil liberties. The NSA did its job—it implemented the authorities it was given.
>
> . . . .
>
> To be clear, I am not saying that citizens should trust the NSA. They should not. Distrust is essential to effective democratic governance. The NSA should be subject to constant and rigorous review, oversight, checks, and balances. The work it does, however important to the safety of the nation, poses grave dangers to fundamental American values, particularly if its work is abused by persons in positions of authority. If anything, oversight of the NSA—especially by Congress—should be strengthened. The future of our nation depends not only on the NSA doing its job, but also on the existence of clear, definitive, and carefully enforced rules and restrictions governing its activities.
>
> In short, I found, to my surprise, that the NSA deserves the respect and appreciation of the American people. But it should never, ever, be trusted.[32]

My second general observation concerns the issue of oversight. On my flight to Washington for the first meeting of the Review Group, I assumed that the absence of oversight was a serious problem. Not only was the NSA running amok, but no one was paying attention. Once again, I was wrong. As a member of the Review Group, I had a rare opportunity to observe and evaluate the various mechanisms our government uses to oversee the activities of our nation's intelligence agencies. At the structural level, I was impressed with the variety and range of oversight mechanisms in place.

The National Security Agency's activities, for example, are overseen by the NSA's Inspector General, the Director of National Intelligence, the FISC, the Department of Justice, the Privacy and Civil Liberties Oversight Board, and the Senate and House Intelligence Committees.[33] Each of these entities is responsible for reviewing various aspects of the NSA's operations.[34] Cumulatively, I found that these oversight mechanisms work reasonably well when it comes to ensuring that the NSA properly implements the

32. *Id.* (in a speech given to the NSA).

33. *Frequently Asked Questions Oversight*, NSA.GOV, https://www.nsa.gov/about/faqs/oversight.shtml (last visited July 9, 2015).

34. *Id.*

authorities it has been given. In those instances in which the NSA overstepped its bounds, these entities were quick to respond.

To cite just one example, in 2009 the FISC learned that the NSA had misapplied a legal standard, resulting in improper access to telephone metadata.[35] Although finding that the noncompliance had been unintentional, the FISC nonetheless prohibited "the government [from] access[ing] the data collected until such time as the government is able to restore the Court's confidence that the government can and will comply with previously approved procedures for accessing such data."[36] The FISC finally lifted this restriction six months later, only after the NSA had demonstrated to the court's satisfaction that the causes of the noncompliance had been corrected and that additional safeguards had been instituted.[37] This is but one example of this type of oversight, but it reflects the seriousness with which the various entities engaged in this process undertake their responsibilities. On balance, they seem to do a reasonable job of ensuring that the intelligence agencies comply with their legal authorities.

I was less impressed, though, with oversight of a different sort. Once the government, whether the Executive Branch, the Congress, or the FISC, authorizes the intelligence agencies to undertake certain types of surveillance, there is insufficient attention to whether the programs instituted under those authorities can and should be refined and improved over time. This sort of retrospective oversight—constantly evaluating and re-evaluating programs to ensure that they are properly designed to respect competing interests in individual privacy and civil liberties—is absolutely essential. The issue here is not whether the intelligence agencies are violating the rules, but whether the rules themselves should be reconsidered.

There is a natural and understandable temptation in the realm of national security to err on the side of granting broad rather than narrow powers to our intelligence agencies, especially in the wake of a crisis.[38] But the reality of this temptation makes it especially important that there be rigorous, on-

35. *In re* Production of Tangible Things from [Undisclosed Service Provider], No. BR 08-13 (FISA Ct. Mar. 2, 2009).

36. *Id.*

37. *In re* Production of Tangible Things from [Undisclosed Service Provider], No. BR 09-13 (FISA Ct. Sept. 25, 2009); CLARKE ET AL., NSA REPORT, *supra* note 27, at 60.

38. *See* Tyler Raimo, Note, *Winning at the Expense of Law: The Ramifications of Expanding Counter-Terrorism Law Enforcement Jurisdiction Overseas*, 14 AM. U. INT'L L. REV. 1473, 1493–94, 1506–08 (1999).

going scrutiny of the programs that have been authorized, because with experience it will often be possible to identify ways in which those programs can be refined and narrowed to strike a better balance between the interests of national security and individual liberty.[39]

That, indeed, was the central theme of the Review Group's 46 recommendations. What we found in program after program was that significant refinements could and should be made that would better protect personal privacy and individual freedom without unduly interfering with the capacity of these programs to keep our nation safe.[40] The fact that an extraordinary and ad hoc institution like the Review Group was necessary to bring these recommendations to the fore strongly suggests that existing oversight mechanisms were not performing this function adequately. This must change in the future.

To that end, I offer three suggestions. First, the Senate and House Intelligence Committees must be staffed by individuals who have deep experience and strong credibility within the intelligence agencies. It quickly became apparent to me that the Review Group would never have been able to do our work successfully if two of our members—Michael Morell and Richard Clarke—had not been deputy director of the Central Intelligence Agency[41] and National Security Council Counterterrorism Coordinator,[42] respectively.

The congressional intelligence committees lack such expertise.[43] If they are to fulfill their responsibilities effectively, they need access to similar expertise and credibility.[44] Indeed, as several members of these committees made clear to me during the review process, the House and Senate Intelligence Committees, as currently staffed, cannot effectively comprehend and oversee the vast complexities of the intelligence community. That needs to change.

39. *See* CLARKE ET AL., NSA REPORT, *supra* note 27, at xvi–xvii; Stone, *What I Told*, *supra* note 31.

40. *See* CLARK ET AL., NSA REPORT, *supra* note 27, at xvii–xxiii.

41. *Executive Profile: Michael J. Morell*, *supra* note 22.

42. THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 255 (authorized ed., 2004) [hereinafter 9/11 REPORT]; *Biography*, *supra* note 23.

43. 9/11 REPORT, *supra* note 42, at 103; Gregory S. McNeal, *Targeted Killing and Accountability*, 102 GEO. L.J. 681, 774 (2014).

44. McNeal, *supra* note 43, at 742–44.

Second, the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) recommended the creation of what is now the Privacy and Civil Liberties Oversight Board (the PCLOB), an independent agency in the Executive Branch designed to conduct oversight of intelligence agency activities and make recommendations to Congress and the Executive Branch about how to improve privacy and civil liberty protections.[45] Unfortunately, the PCLOB has been given too narrow a focus, too few resources, and too little authority to do its job effectively.[46] The Review Group therefore recommended the creation of a new agency to replace the PCLOB that would have a broader focus, more resources, and greater authority to fulfill the essential functions of reviewing and overseeing the activities of the intelligence agencies and reporting regularly on those activities, in both classified and unclassified forms, to both Congress and the public.[47]

Third, given the importance of ongoing oversight of our foreign intelligence activities and the need for a fresh set of eyes to review and analyze these programs periodically to ensure that they strike the right balance between security and liberty, every five years the President should appoint a review group similar to the one on which I had the privilege of serving. By bringing an independent and clear-eyed perspective to the task, such a Review Group can see problems and identify solutions that may be invisible to those who are too close to the programs themselves.[48] In a realm that out of necessity operates in secret, an outside perspective is critical to the government's ability to identify significant, though not always obvious, opportunities for reform.[49]

If there is one lesson to be learned from the reforms now being debated

45. Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 801, 121 Stat. 352–58; 9/11 REPORT, *supra* note 42, at 395 (recommending a board within the executive branch to oversee "the commitment the government makes to defend our civil liberties").

46. Chris Calabrese, *The Limits of Oversight and the PCLOB*, ACLU (May 17, 2012), www.aclu.org/blog/limits-oversight-and-pclob (reviewing the Board's limited resources and lack of subpoena power).

47. *See* CLARKE ET AL., NSA REPORT, *supra* note 27, at 142–46.

48. *Remarks by the President in a Press Conference*, THE WHITE HOUSE (Aug. 9, 2013), https://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference (stating that the reason the Review Group was formed was to "step back and review our capabilities" because the country needs "new thinking for a new era" to help determine how best to combat terrorism while maintaining "the trust of the people").

49. *See id.*

and implemented with respect the activities of our intelligence community, it is that constant, rigorous, and independent review is essential if we are to strike the proper balance between liberty and security in a changing world.[50]

V.

Let me turn now to a few of the Review Group's specific recommendations. The Report contains 46 recommendations, but that understates the number of issues addressed.[51] Many have subparts, so there are about 200 recommendations in all.[52] The recommendations address a broad range of issues, including: foreign intelligence surveillance programs directed at United States persons; foreign intelligence surveillance programs directed at non-United States persons; determining what intelligence should be collected and how; organizational reform in light of changing communications technology; promoting security and openness in the realm of global communications technology; and protecting the information we collect.[53]

To offer a sense of the group's thought processes and President Obama's response to our recommendations, I will focus on three main areas: the collection of telephone metadata; the use of national security letters to obtain private information; and the role of the FISC.

A. *Section 215 Telephony Metadata Program*

Before 1978, when the government engaged in foreign intelligence surveillance, whether in the United States or abroad, such surveillance was subject only to the discretion of the President as Commander in Chief.[54] There was no legislative restriction and there was no judicial involvement in anything the President did in the name of foreign intelligence surveillance.[55] If the President wanted to wiretap a phone call between people in the United States on the belief that it was relevant to foreign intelligence, the President could do that without probable cause, without a warrant, and without any

50. *See* CLARKE ET AL., NSA REPORT, *supra* note 27, at 140–46.

51. *See id.* at xxv–xli.

52. *See generally id.*

53. *See generally id.*

54. *See* Richard Henry Seamon & William Dylan Gardner, *The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L & PUB. POL'Y 319, 330 (2005).

55. *See id.* at 330–31 (discussing legislative and judicial deference to the President in matters of foreign intelligence gathering).

oversight whatsoever outside the executive branch.[56]

In the 1970s, grave abuses by the FBI, the CIA, the NSA, and Army Intelligence, under the auspices of J. Edgar Hoover, Lyndon Johnson, and Richard Nixon, came to light.[57] They had engaged in what was understood to be inappropriate—and in some instances illegal—surveillance of American citizens for a variety of reasons, mostly political, and often highly invasive of privacy beyond the scope of any agency's authority.[58]

Congress instituted the Church Committee, named after Senator Frank Church, to establish oversight of the Executive branch and reign in these abuses.[59] The Church Committee Report,[60] one of the truly great documents in the history of Congress, made a series of complex recommendations, which ultimately resulted in the Foreign Intelligence Surveillance Act of 1978.[61] That legislation did many things, but most importantly, it brought various elements of foreign intelligence surveillance under the rule of law through the creation of the Foreign Intelligence Surveillance Court (FISC).[62]

Ordinary federal courts did not have security clearances, and a great deal of foreign intelligence information was classified.[63] Therefore, an ordinary federal judge could not decide whether the executive branch could undertake a foreign intelligence wiretap.[64] The FISC enabled judges to play their traditional role in overseeing what the Executive Branch did in the classified realm.[65] The court was only authorized to deal with foreign intelligence surveillance that took place inside the United States.[66] What the President

56. *See id.*

57. *See* CLARKE ET AL., NSA REPORT, *supra* note 27, at 12–13.

58. *See* CHURCH COMMITTEE REPORT, *supra* note 19, at 6–10; STONE, PERILOUS TIMES, *supra* note 19, at 496–97; THEOHARIS, *supra* note 19, at 134–36.

59. CLARKE ET AL., NSA REPORT, *supra* note 27, at 14.

60. *See* CHURCH COMMITTEE REPORT, *supra* note 19. For a summary of the key findings of the Church Committee, see CLARKE ET AL., NSA REPORT, *supra* note 27, at 14–20.

61. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783.

62. *Id.* § 103, 92 Stat. at 1788.

63. *See* CLARKE ET AL., NSA REPORT, *supra* note 27, at 22.

64. *See* § 103, 92 Stat. at 1788.

65. *See id.*

66. *See id.*

did outside the United States was regarded as beyond the scope of even Congress's business at that time.[67]

From the late 1970s until 9/11, that process worked reasonably well, and for the most part, people considered it effective.[68] There was obviously a wake-up call on 9/11, and public support grew for granting intelligence agencies greater capacity to prevent such attacks.[69] Congress made a number of modifications to the Foreign Intelligence Surveillance Act in the wake of 9/11 to strengthen the agencies' ability to ferret out information about terrorist activity.[70] One of the provisions was Section 215 of the Foreign Intelligence Surveillance Act,[71] which authorized the agencies to go to the FISC and apply for an order based on reasonable and articulable suspicion that a suspect was engaged in international terrorist activity.[72] If the agencies met this burden, the court could authorize the agency to go to banks, credit card companies, telephone companies, internet companies, etc., and serve the equivalent of a subpoena demanding records about the individual in question.[73]

In 2006, as technology changed, the NSA came to the FISC and proposed a new program to gather telephone metadata from huge numbers of phone calls that took place in the United States[74]—and to hold that data for five years.[75] That metadata consists of phone numbers—every phone number covered by the order, and every number that calls or is called by that

67. *See id.* § 103, 92 Stat. at 1786–88 (providing that the President may authorize electronic surveillance without a court order if only directed at foreign powers and "there is no substantial likelihood that surveillance will acquire the contents of any communication to which a United States person is a party").

68. 9/11 REPORT, *supra* note 42, at 104 (finding terrorism was not a concern of the public prior to 9/11).

69. CHICAGO COUNCIL ON GLOBAL AFFAIRS, FOREIGN POLICY IN THE NEW MILLENNIUM 1 (2012) ("In 2002 . . . Americans were ready to allocate almost unlimited attention and resources to countering the terrorist threat.").

70. *See generally* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (codified as amended at 50 U.S.C. § 1861(a)(1) (2006 & Supp. V 2011)).

71. *See id.*

72. CLARKE ET AL., NSA REPORT, *supra* note 27, at 36–37; *see also In re* Production of Tangible Things from [Redacted], No. BR 08-13, 2009 WL 9150913, at *1 (FISA Ct. 2009).

73. *See* CLARKE ET AL., NSA REPORT, *supra* note 27, at 36.

74. *In re* Production of Tangible Things from [Redacted], 2009 WL 9150913, at *1.

75. CLARKE ET AL., NSA REPORT, *supra* note 27, at 51.

number.[76] It does not include names, it does not include geographical locations, and it does not include content, but it involves huge amounts of numbers.[77]

The intelligence agencies wanted this information because they now had the technological capability to manage a database of that magnitude.[78] The FISC, the Senate and House Intelligence Committees, and the Department of Justice approved the program.[79] It enabled the NSA, when it had reasonable and articulable suspicion that a particular telephone number—almost invariably a number outside the United States—was associated with a person suspected of terrorist activity, to query the database.[80] That is, an NSA analyst could type in the phone number of the suspected terrorist, and the database would spit out information about the numbers with which the suspect's number was in contact.[81]

The idea was to connect the dots.[82] Although the program collected massive amounts of data, it was carefully designed not to reveal that data to the NSA indiscriminately.[83] When the analysts queried a suspected number, the information they received reflected only the numbers associated with other suspected terrorists that the queried number contacted.[84] The goal, in other words, was to determine whether a suspected terrorist outside the United States was speaking to a suspected terrorist inside the United States.[85]

In 2012, the most recent year for which full data was then available, the NSA queried the database for 288 numbers.[86] Those 288 numbers yielded 12 tips.[87] That is, in 12 instances based on those 288 queries, agents discovered

76. *Id.* at 49–51.

77. *Id.* at 50 (quoting *In re* Application of the Federal Bureau of Investigations for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109 (FISA Ct. 2013).

78. *See* WHITE PAPER, Bulk Collection of Telephony Meta-data Under Section 215 of the USA PATRIOT Act, 1 (August 9, 2013) [hereinafter WHITE PAPER].

79. *See id.* at 5.

80. CLARKE ET AL., NSA REPORT, *supra* note 27, at 52.

81. *See* WHITE PAPER, *supra* note 78, at 3.

82. *See id.* at 2–3.

83. *Id.* at 3; CLARKE ET AL., NSA REPORT, *supra* note 27, at 52–55.

84. CLARKE ET AL., NSA REPORT, *supra* note 27, at 52.

85. WHITE PAPER, *supra* note 78 at 3.

86. CLARKE ET AL., NSA REPORT, *supra* note 27, at 56.

87. *Id.* at 57.

that the suspected terrorists outside the United States were communicating with numbers associated with terrorist suspects in the United States.[88] In those 12 instances, the NSA turned the information over to the FBI for further investigation.[89]

None of the 12 tips in 2012 produced information that was useful in preventing a planned terrorist attack.[90] In fact, the Review Group's findings suggested that, in the seven years in which the program existed, there had not been a single instance in which the metadata program led directly to the prevention of a terrorist attack.[91] Many other programs employed by the NSA had very productive results, but not this one.[92]

Defenders of the program argued, I think persuasively, that the fact that the program had yet to turn up information that prevented a terrorist attack did not represent a failure.[93] An effort to prevent attacks on the scale of 9/11—such as nuclear, chemical, biological attacks—might yield meaningful information only once in a decade. Failing to prevent such an attack, though, would be catastrophic. Thus, the program was analogous to a fire alarm in one's home. It might save your life only once a decade, but that doesn't mean you toss it out.

In evaluating the program, we determined that it was not as draconian as the public has been led to believe. It is much more carefully targeted and managed, and its potential value is real.[94] Nevertheless, we concluded that the program was not limited adequately to protect the legitimate privacy interests of Americans.[95] With that in mind, we made three fundamental recommendations with regard to the program:

1. *The Government Should Not Hold the Database*

Historical experience teaches that one grave danger is the risk of some

88. *See id.*
89. *Id.*
90. *See id.*
91. *Id.*
92. *Id.*
93. *See* John Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, 37 HARV. J.L. & PUB. POL'Y 901, 909–12, 929–30 (2014) (discussing the benefits this data can provide to the intelligence community to be used to stop future attacks).
94. *See* CLARKE ET AL., NSA REPORT, *supra* note 27, at 52–55.
95. *See id.* at 58–61.

misguided public official—whether a J. Edgar Hoover or a Richard Nixon—using this extraordinary data to do harm or to learn information about free speech, political associations, or political enemies.[96] Although the metadata consists only of phone numbers, if you look at the pattern of a person's calls over an extended period of time, you can learn a lot about that person that can be put to nefarious use.[97] Therefore, we recommended that the information should remain in the hands of the telephone service providers, who already have it for billing purposes.[98] But the government itself should not hold the data.[99]

2. *The NSA Should Not be Able to Query the Database Without a Court Order*

Human nature being what it is, the people engaged in the enterprise of finding bad people are likely to err on the side of suspicion where a neutral or detached observer might not.[100] That is why the United States ordinarily requires search warrants issued by neutral and detached judges in criminal investigations.[101] We therefore recommended that the NSA should not be

96. *See id.* at 11–12.

97. *See id.* at 68–69 (stating that data who someone is calling can reveal a "wealth of detail" about the person's various associates, whether they be familial, religious, political, and even sexual, and can reveal whether the person made calls to psychiatrists, sexually transmitted disease treatment facilities, criminal defense attorneys, etc. (quoting United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring))).

98. CLARKE ET AL., NSA REPORT, *supra* note 27, at 67.

99. *Id.*

100. *See, e.g.*, *id.* at 64–65 (discussing the dangers of "false positives" in the hunt for terrorists).

101. *See, e.g.*, California v. Acevedo, 500 U.S. 565, 586 (1991) (recognizing that the Fourth Amendment is an important restraint "against police practices that prevail in totalitarian regimes" and that the "decision to invade the privacy of an individual's personal effects should be made by a neutral magistrate rather than an agent of the Executive"); Johnson v. United States, 333 U.S. 10, 13–14 (1948) ("The point of the Fourth Amendment, which is often not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. Any assumption that evidence sufficient to support a magistrate's disinterested determination to issue a search warrant will justify the officers in making a search without a warrant would reduce the [Fourth] Amendment to a nullity and leave people's homes secure only in the discretion of police officers."); Fabio Arcila, Jr., In re *Trenches: Searches and the Misunderstood Common-Law History of Suspicion and Probable Cause*, 10 U. PA. J. CONST. L. 1, 9–16 (2007) (discussing the

allowed to query the database on the basis of its own analysts' judgment.[102] The FISC should have to determine independently and individually whether the standard of reasonable and articulable suspicion is met.[103] This requirement would also substantially reduce the risk of unlawful access to the database.[104]

3. *The Data Should Not be Held for More Than Two Years*

We concluded that five years is unnecessary.[105] The data gets stale, its value depreciates, and the risks of misuse increase as the information accumulates.[106]

These recommendations were all incorporated into the USA Freedom Act, which was adopted by Congress and signed into law by President Obama on June 2, 2015.[107]

B. *National Security Letters*

Another recommendation involved an investigatory tool called national security letters (NSLs).[108] In another post-9/11 action, the government authorized the FBI to issue NSLs when, in the course of a national security investigation, it wanted to obtain information such as bank records, credit card records, telephone records, and travel records about a person it suspects of being involved in terrorist activity.[109] Using these letters, the FBI itself issued such orders to the companies directing them to turn over the relevant information.[110]

NSLs have been controversial ever since they came into existence, in part because they are highly secretive.[111] The process is classified and there

Founders' experience with writs of assistance and general warrants which were the reasoning behind the drafting of the Fourth Amendment).

102. *See* CLARKE ET AL., NSA REPORT, *supra* note 27, at 47, 67.

103. *Id.*

104. *Id.* at 65–69 (discussing the potential ways government officials and analysts could misuse the data without proper safeguards).

105. *Id.* at 70 n.118.

106. *See id.* at 65–66.

107. *See* USA Freedom Act of 2015, Pub. L. No. 114-23, 129 Stat. 268.

108. *See* CLARKE ET AL., NSA REPORT, *supra* note 27, at 43–44, 73–75.

109. *See id.* at 44–47.

110. *See id.*; 12 U.S.C. § 3414 (2012); 15 U.S.C. § 1681(u), (v) (2012); 18 U.S.C. § 2709 (2012); 50 U.S.C. § 436 (2012).

111. *See* CLARKE ET AL., NSA REPORT, *supra* note 27, at 46–47.

have been abuses in the use of NSLs, which have been reported to Congress.[112] Although the abuses have been addressed in various ways, they have been a source of some concern.[113] Our view was that, in the absence of a situation where time spent going before a judge would pose a danger to the nation, a court order should be required for the use of NSLs.[114]

When we discussed this issue with the FBI, it adamantly opposed this recommendation. Its view was that the inefficiency of such a requirement would interfere with the prompt use of NSLs. Moreover, it argued that there was no reason why the government should be forced to jump through more hoops in a terrorist investigation than, say, a prosecutor would have to jump through in a drug investigation.[115]

The Review Group argued there is a big difference between the use of subpoenas and the use of NSLs.[116] Subpoenas are largely transparent.[117] They are not classified or secret.[118] They are often at issue in criminal prosecutions when the government wants to introduce evidence, and their legality can therefore be openly challenged. The NSLs, on the other hand, are classified.[119] Rather than being able to challenge its legality in court, a phone company or a bank that receives an NSL cannot say anything about it, under

112. *See, e.g.*, U.S. DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS IN 2006, AT 59–64 (2008); DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 2:17, § 20 (West 2014).

113. *See* CLARKE ET AL., NSA REPORT, *supra* note 27, at 46–47.

114. *See id.* at 43–44 (recommending that NSAs should be issued "only upon a judicial finding that: (1) the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect 'against international terrorism or clandestine intelligence activities' and (2) like a subpoena, the order is reasonable in focus, scope, and breadth").

115. During a drug investigation, a prosecutor can issue a subpoena, which functions in much the same way as an NSL, without judicial approval. *See, e.g.*, U.S. DEP'T OF JUSTICE OFFICE OF LEGAL POLICY, REPORT TO CONGRESS ON THE USE OF ADMINISTRATIVE SUBPOENA AUTHORITIES BY EXECUTIVE BRANCH AGENCIES AND ENTITIES 6–9 [hereinafter ADMINISTRATIVE SUBPOENA], *available at* http://www.justice.gov/archive/olp/rpt_to_congress.pdf (outlining the sources of administrative subpoena power and the exercise of that authority).

116. *See, e.g.*, CLARKE ET AL., NSA REPORT, *supra* note 27, at 46 n.76.

117. *See* ADMINISTRATIVE SUBPOENA, *supra* note 115, at 18–26 (outlining the various protections and disclosure requirements governing administrative subpoenas and subpoenaed information).

118. *Id.*

119. *See* CLARKE ET AL., NSA REPORT, *supra* note 27, at 45.

threat of criminal prosecution.[120]

We considered that lack of transparency a serious problem that invites the kind of abuse that we were charged with preventing.[121] The absence of a judicial check creates an inevitable temptation to err on the side of finding suspicion where it does not exist.[122] On this score, President Obama did not accept our recommendation to require a court order for the issuance of NSLs.[123]

C. *Foreign Intelligence Surveillance Court*

A third issue involved the operations of the FISC. The FISC was designed primarily to issue search warrants and to limit the ability of presidents to authorize foreign intelligence wiretaps in the United States without judicial oversight.[124] With the enactment of the Foreign Intelligence Surveillance Act of 1978, the government would have to establish probable cause before a judge on the FISC would issue a warrant, even for the purpose of foreign intelligence surveillance.[125]

What became evident over time, though, was that on rare occasions the FISC would have to decide not only whether the government could show probable cause for a particular investigation, but also whether and how the law governed certain novel methods of surveillance.[126] Sometimes these involved complex questions of statutory or constitutional interpretation.[127] This was illustrated by the FISC's decision to permit the Section 215 metadata program.[128]

The Review Group's judgment was that when such issues arise, the FISC judges should hear arguments not only from the government, but also

120. *See id.*

121. *See id.* at 73–80.

122. *See id.* at 46–48.

123. *See* President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014) [hereinafter Signals Intelligence], *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

124. CLARKE ET AL., NSA REPORT, *supra* note 27, at 22.

125. *Id.*

126. *Id.* at 149.

127. *Id.*

128. *See In re* Application of the F.B.I. for an Order Requiring the Prod. of Tangible Things from [Telecomms. Providers] Relating to [Redacted], No. BR-05 (FISA Ct. May 24, 2006); CLARKE ET AL., NSA REPORT, *supra* note 27, at 48.

from advocates for the other side, just as would any other court.[129] We therefore recommended the creation of a privacy and civil liberties advocate to represent the other side on these sorts of complex legal and constitutional issues.[130] The FISC judges objected to this recommendation.[131] They argued that they were responsible jurists who could sort through the legal issues on their own.[132]

President Obama compromised on this. He adopted the recommendation that there should be a privacy and civil liberties advocate, but he concluded that this advocate should be authorized to participate in the proceedings of the FISC only if the judges of that court invited such participation.[133] This recommendation is also incorporated into the USA Freedom Act.[134]

VI.

In the end, this was a truly extraordinary experience. Not only did it provide my colleagues on the review group and me with remarkable insights into the inner workings of our national security state, but it also resulted—somewhat to my surprise—in a series of important and far-reaching recommendations that, with the enactment of the USA Freedom Act, have helped to shape the structure and operation of many of these programs.[135]

129. *See* CLARKE ET AL., NSA REPORT, *supra* note 27, at 148–50.

130. *See id.*

131. *See* Ellen Nakashima, *Surveillance-Court Judges Oppose White House Group's NSA Proposals*, WASH. POST (Jan. 14, 2014), https://www.washingtonpost.com/world/national-security/surveillance-court-judges-oppose-white-house-groups-nsa-proposals/2014/01/14/3c41e1e2-7d60-11e3-93c1-0e888170b723_story.html.

132. *See id.*

133. *See* Signals Intelligence, *supra* note 123 (calling on Congress to "authorize the establishment of a panel of advocates from outside government to provide an independent voice in significant cases before the [FISC]").

134. *See* USA Freedom Act of 2015, Pub. L. No. 114-23, § 401, 129 Stat. 268, 279–81.

135. *See generally id.* 129 Stat. 268; CLARKE ET AL., NSA REPORT, *supra* note 27.